

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-107082

(43) 公開日 平成7年(1995)4月21日

(51) Int.Cl.<sup>6</sup>

H 0 4 L 9/00

9/10

9/12

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/00

Z

審査請求 未請求 請求項の数1 OL (全13頁)

(21) 出願番号 特願平5-250850

(22) 出願日 平成5年(1993)10月6日

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72) 発明者 山口 利和

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(74) 代理人 弁理士 伊東 忠彦

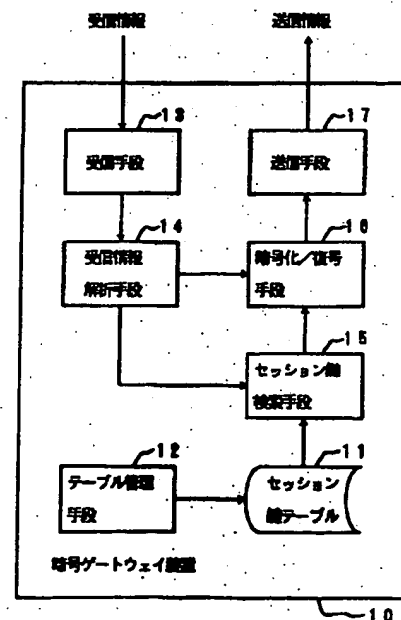
(54) 【発明の名称】 暗号ゲートウェイ装置

(57) 【要約】

【目的】 本発明は、暗号化／非暗号化の選択及びセッション鍵の選択を端末の組合せ毎又はセッション毎に設定し、既存の端末装置のハードウェア及びアプリケーションプログラムに影響を与えることなく暗号通信を実現する暗号ゲートウェイ装置を提供することを目的とする。

【構成】 本発明の暗号ゲートウェイ装置は、端末の識別情報とセッション鍵の組を保持するセッション鍵テーブル(11)と、上記組をセッション鍵テーブルに登録する手段(12)と、受信情報から端末識別情報と通信文を抽出する手段(14)と、識別情報を検索キーとしてセッション鍵テーブルからセッション鍵を検索する手段(15)と、識別情報とセッション鍵に応じて通信文を暗号化又は復号する手段(16)とから成り、セッション鍵の検索の結果該当するセッション鍵が無い場合には通信文を原文のまま送信する構成を特徴とする。

本発明の構成図



## 【特許請求の範囲】

【請求項 1】 受信情報を送信端末から受信し、該受信情報を暗号化又は復号し、該暗号化又は復号された送信情報を受信端末に送信する暗号ゲートウェイ装置において、

送信端末及び受信端末の識別情報と該暗号化又は復号のためのセッション鍵の組を保持するセッション鍵テーブルと、

前記送信端末及び受信端末の識別情報と該セッション鍵を該セッション鍵テーブルに登録するテーブル管理手段と、

前記受信情報から前記送信端末及び受信端末の識別情報と、通信文を抽出する受信情報解析手段と、

該抽出された識別情報を検索キーとして前記セッション鍵テーブルから該当するセッション鍵を検索するセッション鍵検索手段と、

前記抽出された識別情報と前記該当するセッション鍵に応じて該通信文を暗号化又は復号して送信情報を作成する暗号化復号手段とから成り、

上記セッション鍵検索手段による検索の結果前記セッション鍵テーブルに該当するセッション鍵が無い場合には前記通信文を原文のまま送信する構成としたことを特徴とする暗号ゲートウェイ装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は暗号ゲートウェイ装置に係り、特に広い地域に分散した事業所等の特定グループ内の端末間で暗号通信を行う場合に、任意の 2 台の端末が共通のセッション鍵を有することにより暗号通信を行うパケット通信システムにおける暗号ゲートウェイ装置に関する。

## 【0002】

【従来の技術】 図 10 は従来技術による暗号通信システムを説明する図であって、端末 i 130 と端末 j 140 との間で通信を行う場合、一方の端末 i 130 のアプリケーションプログラム 132 (以下、AP と略す) が鍵配送センタ 160 から通信に使用するセッション鍵 162 を取得する。端末 i 130 の AP 132 は、このセッション鍵を通信相手の端末 j 140 に送信して、2 台の端末で共通のセッション鍵を共有し、これを用いて通信文を暗号化及び復号して暗号通信を行う。

【0003】 図 11 は、従来の暗号ゲートウェイ装置 180 を説明する図であって、暗号化／復号を行うための固定セッション鍵 181 と、受信情報を受信するための受信部 182 と、受信情報を解析して通信文を抽出する受信情報解析部 183 と、固定セッション鍵 181 を利用して通信文を暗号化／復号する暗号化／復号部 184 と、暗号化／復号された通信文を送信する送信部 185 とから成る。

【0004】 図 12 は、図 11 に示す暗号ゲートウェイ

装置を利用した暗号通信システムを説明するための図であり、端末 211、212、...、21n から成る A グループの端末に暗号ゲートウェイ装置 180<sub>1</sub> が外付けされ、端末 311、312、...、31n から成る B グループの端末に暗号ゲートウェイ装置 180<sub>2</sub> が外付けされる。暗号ゲートウェイ装置 180<sub>1</sub>、180<sub>2</sub> のセッション鍵は固定であるため、端末 211 と端末 312 の暗号通信と、端末 21n と端末 312 の暗号通信とは共通のセッション鍵で暗号化される。さらに、例えば、端末 212 と端末 311 との通信のように暗号化が不要な通信を行う場合には、暗号ゲートウェイ装置 180<sub>1</sub> と 180<sub>2</sub> とを介さない伝送路を用いて通信を行う。

## 【0005】

【発明が解決しようとする課題】 図 10 に示す従来の暗号通信システムでは、暗号通信に先立って、一方の端末上の AP が鍵配送センタからセッション鍵を取得し、これを通信相手の端末に送信することが必要であって、端末の AP 側の処理が煩雑である。

【0006】 さらに、平文による端末間の通信を暗号通信に対応するよう変更するためには、端末装置のハードウェア又は AP を個別に改造する必要があるが、通信システムにおける端末の種類と AP は膨大な数に及ぶので、改造の規模及び工数が大きく、従って開発費も大きくなるという問題がある。

【0007】 一方、従来の暗号ゲートウェイ装置を利用する場合には、固定のセッション鍵により画一的に暗号化又は復号がなされるため、通信相手先の端末が暗号通信を行うか、或いは非暗号化通信を行うかに応じて暗号通信のセッション鍵の変更等を行うことができない。

【0008】 本発明は上記の従来の暗号通信システムの問題点に鑑み、暗号通信と非暗号通信の選択と、暗号通信における共有セッション鍵の選択を端末の組合せ毎又はセッション毎に設定し、さらに、既存の端末装置のハードウェア及び AP に影響を与えることなく暗号通信を実現する暗号ゲートウェイ装置を提供することを目的とする。

## 【0009】

【課題を解決するための手段】 図 1 は本発明の原理構成図である。本発明の暗号ゲートウェイ装置は、受信情報を送信端末から受信し (13)、該受信情報を暗号化又は復号し、該暗号化又は復号された送信情報を受信端末に送信して (17) 暗号通信を行う装置であって、送信端末及び受信端末の識別情報と暗号化又は復号のためのセッション鍵の組を保持するセッション鍵テーブル (11) と、送信端末及び受信端末の識別情報とセッション鍵をセッション鍵テーブルに登録するテーブル管理手段 (12) と、受信情報から送信端末及び受信端末の識別情報と、通信文を抽出する受信情報解析手段 (14) と、抽出された識別情報を検索キーとしてセッション鍵

テーブルから該当するセッション鍵を検索するセッション鍵検索手段(15)と、抽出された識別情報と該当するセッション鍵に応じて通信文を暗号化又は復号して送信情報を作成する暗号化復号手段(16)とから成り、セッション鍵検索手段による検索の結果セッション鍵テーブルに該当するセッション鍵が無い場合には通信文を原文のまま送信する構成を特徴とする。

【0010】

【作用】本発明の暗号ゲートウェイ装置は、送信端末と受信端末の組合せ毎又はセッション毎に暗号化用セッション鍵を選定してセッション鍵テーブルを構成し、送信端末から受信した情報により送信元と送信先を識別し、その識別結果をキーとしてセッション鍵テーブルを検索してセッション鍵を得て送信情報の通信文を暗号化又は復号し、セッション鍵が得られない場合には原文のまま送信用通信文として受信端末に送信する。したがって、送信端末から送られた通信文が暗号文と平文のいずれであっても受信することができる。さらに、セッション鍵テーブルを用いることによりセッション鍵を送信端末と受信端末の組合せ毎又はセッション毎に自由に設定できるので、既存の端末に接続する際に、既存の端末ハードウェア、及び、端末のAPを改造する必要がない。

【0011】図2は本発明の暗号ゲートウェイ装置を利用した暗号通信システムの概要を説明する図であり、伝送路40と、Aグループの端末21<sub>1</sub>、...、21<sub>n</sub>と、Bグループの端末31<sub>1</sub>、...、31<sub>n</sub>と、Cグループの端末32<sub>1</sub>、...、32<sub>1</sub>とから成る通信システムにおいて、Aグループに暗号ゲートウェイ装置Aを、Bグループに暗号ゲートウェイ装置Bをさらに設置している。本発明の暗号ゲートウェイ装置により、暗号化と復号が端末の識別情報に応じて判別され、即ち、暗号ゲートウェイ装置が接続されている端末からの送信は暗号化され、暗号ゲートウェイ装置が接続されている端末への送信情報は復号される。さらに、セッション鍵テーブルにセッション鍵が登録されていないセッションに対する通信は、通信文の原文のまま、即ち、平文で通信される。

【0012】ここで、全ての端末が平文のみを送受信する端末とし、AグループとBグループの間は暗号通信を行ない、CグループとAグループ及びCグループとBグループとは非暗号通信を行うことを考える。まず最初に、Aグループの暗号ゲートウェイ装置A20のセッション鍵テーブルに、Aグループの端末21<sub>1</sub>、...、21<sub>n</sub>を送信元とし、Bグループの端末31<sub>1</sub>、...、31<sub>n</sub>を送信先とするセッションに対するセッション鍵を登録する。本発明の暗号ゲートウェイ装置により、暗号ゲートウェイ装置が接続されている端末からの送信は暗号化を行うので、暗号ゲートウェイ装置A20は、Aグループ内の端末からBグループの端末への送信情報を暗号化して伝送路40に出力する。次

に、Bグループの暗号ゲートウェイ装置B30のセッション鍵テーブルにも同様に、Aグループの端末21<sub>1</sub>、...、21<sub>n</sub>を送信元とし、Bグループの端末31<sub>1</sub>、...、31<sub>n</sub>を送信先とするセッションに対するセッション鍵を登録する。本発明の暗号ゲートウェイ装置により、暗号ゲートウェイ装置が接続されている端末への送信情報は復号するので、暗号ゲートウェイ装置B30は、Aグループ内の端末からBグループの端末への送信情報を復号してBグループ内の端末に出力する。以上により、Aグループ内の端末からBグループBの端末への通信は、各グループ内では平文であって、暗号ゲートウェイ装置を介した伝送路上の通信は暗号文とすることができる。尚、上記と同様にして、Bグループの端末31<sub>1</sub>、...、31<sub>n</sub>を送信元とし、Aグループの端末21<sub>1</sub>、...、21<sub>n</sub>を送信先とするセッションに対するセッション鍵をAグループの暗号ゲートウェイ装置A20のセッション鍵テーブル及びBグループの暗号ゲートウェイ装置B30のセッション鍵テーブルに登録することにより、Bグループ内の端末からAグループ内の端末への通信を暗号通信化できるようになる。

【0013】一方、Aグループの暗号ゲートウェイ装置A20のセッション鍵テーブル及びBグループの暗号ゲートウェイ装置B30のセッション鍵テーブルには、Cグループの端末とにより形成するセッションの登録は行わない。本発明の暗号ゲートウェイ装置により、セッション鍵テーブルにセッション鍵が登録されていないセッションに対しては、平文のまま通信するので、AグループとCグループとの通信及びBグループとCグループとの通信は、平文で行われる。

【0014】次に、端末21<sub>1</sub>、21<sub>n</sub>、31<sub>2</sub>は、暗号文のみを送受信する端末とし、端末21<sub>2</sub>、31<sub>1</sub>、31<sub>n</sub>を平文のみを送受信する端末として、本発明の暗号ゲートウェイ装置を説明する。ここで、暗号ゲートウェイ装置A20のセッション鍵テーブルには、送信元が端末21<sub>2</sub>であって、送信先がBグループ内の各端末31<sub>1</sub>、...、31<sub>n</sub>であるセッションと、送信元がBグループBの各端末31<sub>1</sub>、...、31<sub>n</sub>であり、送信先が端末21<sub>2</sub>であるセッションに対してセッション鍵を登録する。これにより、端末21<sub>2</sub>からの通信文は暗号ゲートウェイ装置A20により暗号化され、端末21<sub>1</sub>、21<sub>n</sub>からの通信文は原文、即ち暗号文のまま通過される。したがって、送信元の端末に係わらず、暗号ゲートウェイ装置A20は、伝送路40に暗号文を送出する。さらに、暗号ゲートウェイ装置B30のセッション鍵テーブルも同様に設定することにより、暗号ゲートウェイ装置B30から伝送路40に送出される通信文は、すべて暗号文とすることができる。したがって、伝送路40上の通信文はすべて暗号文である。上記の通り、伝送路40を介してグループBの端末から暗号ゲートウェイ装置A20が受信する受信情報は、すべて暗号

5

文である。ここで、暗号ゲートウェイ装置A20は、セッション鍵テーブルに登録された送信先が端末212であるセッションに対する通信文に対応するセッション鍵を用いて復号、即ち平文に変換して端末212に送出する。また、送信先が端末212以外のセッションに対するセッション鍵はセッション鍵テーブルに登録されていないので、暗号ゲートウェイ装置A20は、送信先が端末212以外の通信文は、原文、即ち暗号文のまま送信先に送出する。

【0015】

【実施例】以下、コネクション型のプロトコルを利用してネットワークを介して通信を行うTCP/IP・LAN環境を例として、本発明の一実施例による暗号ゲートウェイ装置の説明を行う。

【0016】図3は本発明の一実施例の暗号ゲートウェイ装置による暗号通信システムの構成図であり、暗号ゲートウェイ装置110と、端末1130と、端末1140と、ネットワーク120から成る。端末1130と端末1140とが、セッションを確立してネットワーク120を介して通信を行う。ここで、端末1130と暗号ゲートウェイ装置110は、ネットワーク120を介して暗号文による通信を行ない、端末1140と暗号ゲートウェイ装置110は、平文による通信を行うものとする。

【0017】暗号ゲートウェイ装置110は、セッション識別子とセッション鍵の組を保持するセッション鍵テーブル111と、セッション鍵テーブル111にセッション鍵を登録するテーブル管理部112と、情報を受信する受信部113と、受信された情報を解析するパケット解析部114と、解析された受信情報に含まれるセッション識別子に対応するセッション鍵をセッション鍵テーブル111から検索するセッション鍵検索部115と、解析された受信情報中の通信文を暗号文又は平文に変換する暗号化/復号部116と、暗号化/復号部116で変換された通信文又はパケット解析部114からの原文のままの通信文を送信する送信部117とから成る。

【0018】図4は、本発明の一実施例によるセッション鍵テーブル111を示し、セッションを識別するためのセッション識別子とそのセッション固有のセッション鍵とを保持する。セッション識別子は、送信元及び送信先のネットワーク内でのアドレスを示すための情報であって、送信元のIPアドレスとポート番号、及び送信先のIPアドレスとポート番号とにより構成される。

【0019】暗号通信を開始する前に、テーブル管理部112が、CRT/KB等の入出力装置、ディスク、又はネットワーク等を介して入力されたセッション識別子とセッション鍵とをセッション鍵テーブル111に登録する。

【0020】セッション鍵テーブル111に登録された

6

セッション識別子を用いて各セッションを一意に識別することができるので、セッション鍵検索部115はこのセッション識別子を検索キーとしてセッション鍵を検索することができる。

【0021】図5は、本発明の一実施例によるTCP/IP・LANで使用するOSIの参照モデルに準拠したプロトコルであって、データリンクレイヤがMAC(Media Access Control)プロトコル、ネットワークレイヤがIP(Internet Protocol)、トランスポートレイヤがTCP(Transmit Control Protocol)で実現され、AP(アプリケーションプログラム)は、TCPレイヤ間でセッションを確立する。本発明の一実施例において、APの通信文(APデータ)に暗号をかけることにより、IPルータを介したネットワークを使用した通信が可能である。

【0022】図6は、本発明の一実施例においてTCP/IP・LANに接続された2台の端末間で通信する際に使用されるパケットのフォーマットを示す図である。パケットは、MACヘッダ(MAC\_H)と、IPヘッダ(IP\_H)と、TCPヘッダ(TCP\_H)から構成されるヘッダと、APデータ及びパケット全体のフレーム・チェック・シーケンス(FCS)から構成される。APデータが暗号化又は復号されて暗号通信が行われる。

【0023】図7は、本発明の一実施例によるIPヘッダのフォーマットを示す図であって、IPヘッダの長さ(単位は4オクテット)を示すIHL(インターネット・ヘッダ長)と、IPヘッダとIPデータ(両者を合わせてIPデータグラムという)を加えたオクテット長を示すTL(全長)と、上位層として利用されるプロトコル(本発明の一実施例ではTCPプロトコルであって、値は'6')を示すPROT(プロトコル)と、送信元IPアドレスを示すSRC\_ADDR(ソース・アドレス)と、送信先IPアドレスを示すDST\_ADDR(デスティネーション・アドレス)とより成る。尚、図中に'-'で示された上記以外のIPヘッダの項目については説明を省略するが、IPヘッダの詳細は、「道下、本間：異機種接続とTCP/IP絵とき読本、オーム社」に記載されている。

【0024】パケット解析部114は、IHLにより上位プロトコル(本発明の一実施例ではTCPプロトコル)のヘッダ開始位置を識別する。暗号化/復号部116は、TLによりAPデータの末尾、即ち暗号化/復号処理の終了位置を識別する。

【0025】図8は、本発明の一実施例によるTCPヘッダのフォーマットを示す図であって、送信元のポート番号を表すSRC\_PORT(ソース・ポート)と、送信先のポート番号を表すDST\_PORT(デスティネーション・ポート)と、TCPヘッダ長(単位は4オクテット)を示すDO(データ・オフセット)から成る。

暗号化/復号部116は、DOの値によりAPデータの開始位置、即ち暗号化/復号処理の開始位置を識別する。

【0026】以下では、図3に示すシステムにおいて、受信されたパケットに応じて、端末1130から端末j140へのAPデータは復号し、端末j140から端末i130へのAPデータは暗号化し、端末j140が送信元又は送信先に指定された上記以外のAPデータは通過（非暗号化）し、その他のパケットは無視するように実現された本発明の暗号ゲートウェイ装置110の一実施例を詳細に説明する。

【0027】図9は、本発明の一実施例による暗号ゲートウェイ装置110の暗号化/復号処理を説明するフローチャートである。

【0028】ステップ100）受信部113は、端末i130と端末j140との間で通信されるパケットを受信し、受信パケットをパケット解析部114に送出する。

【0029】ステップ110）パケット解析部114は、受信部113より受信パケットを受信し、受信パケットのMACヘッダからTYPE（タイプ）を取り出し、上位プロトコルがIP（値は0x0800）で無い場合には、受信パケットを送信パケットとして送信部117に転送し、ステップ270に進む（非暗号通信となる）。

【0030】ステップ120）パケット解析部114は、受信パケットのIPヘッダからPROT（プロトコル）を取り出し、上位プロトコルがTCP（値は6）でない場合には、受信パケットを送信パケットとして送信部117に転送し、ステップ270に進む（非暗号通信となる）。

【0031】ステップ130）パケット解析部114は、受信パケットのIPヘッダからTL（全長）を取り出し、この値からIPデータグラム（IPヘッダ、TCPヘッダ、及びAPデータ）を取得する。

【0032】ステップ140）パケット解析部114は、受信パケットのIPヘッダからIHL（インターネット・ヘッダ長）を取り出し、この値に基づいて、IPデータグラムからIPヘッダとIPデータ（TCPヘッダとAPデータ）とを分離する。

【0033】ステップ150）パケット解析部114は、TCPヘッダからDO（データ・オフセット）を取り出し、この値に基づいて、IPデータからAPデータを分離する。

【0034】ステップ160）パケット解析部114は、IPヘッダからSRC\_ADDR（ソース・アドレス）及びDST\_ADDR（デスティネーション・アドレス）を取得する。

【0035】ステップ170）パケット解析部114は、TCPヘッダからSRC\_PORT（ソース・ポート）及びDST\_PORT（デスティネーション・ポート）を取得する。

【0036】ステップ180）セッション鍵検索部115は、セッション識別子、即ち、SRC\_ADDRと、DST\_ADDRと、SRC\_PORTと、及びDST\_PORTをパケット解析部114より入力し、入力したセッション識別子をキーとしてセッション鍵テーブル111を検索する。

【0037】ステップ190）セッション鍵検索部115は、セッション鍵テーブル111に上記セッション識別子が登録されていない場合には、パケット解析部114の受信パケットを送信パケットとして送信部117に転送し、ステップ270に進む（非暗号通信となる）。

【0038】ステップ200）セッション鍵検索部115は、セッション鍵テーブル111から検索されたセッション鍵Ksを取得する。

【0039】ステップ210）暗号化/復号部114は、パケット解析部114の受信パケット、セッション識別子及びAPデータと、セッション鍵検索部のセッション鍵Ksと、さらに、暗号ゲートウェイ装置110が接続されている端末j140のIPアドレス（IPj）を取得する。

【0040】ステップ220）暗号化/復号部114は、上記IPjとセッション識別子中のSRC\_ADDRとを比較して、当該受信パケットの送信方向、即ち、暗号化と復号のいずれであるかを特定する。IPjとSRC\_ADDRが一致する場合、ステップ250に進む。

【0041】ステップ230）暗号化/復号部114は、上記IPjとセッション識別子中のDST\_ADDRとを比較して、当該パケットの送信方向、即ち、暗号化と復号のいずれであるかを特定する。IPjとDST\_ADDRが一致する場合、ステップ260に進む。

【0042】ステップ240）当該受信パケットは、暗号ゲートウェイ装置に接続される端末j140とは無関係であるため、暗号化/復号部114は、当該受信パケットを破棄し、パケット受信に伴う一連動作を終了する。

【0043】ステップ250）暗号化/復号部36は、APデータをセッション鍵Ksを用いて暗号化し、APデータが暗号化された送信パケットを作成し、送信部117に転送し（端末j140から端末i130への暗号化通信）、ステップ270に進む。

【0044】ステップ260）暗号化/復号部36は、APデータをセッション鍵Ksを用いて復号し、APデータが復号された送信パケットを作成し（端末i130から端末j140への復号通信）、送信部117に転送する。

【0045】ステップ270）送信部117は、送信パケットを端末i130又は端末j140に送信し、パケ

ット受信に伴う一連動作を終了する。

【0046】尚、上記本発明の一実施例による説明では受信パケット及び送信パケットを各部の間で転送するものとして説明しているが、受信パケット及び送信パケットをバッファに格納し、格納されるアドレスを転送する等、受信パケット及び送信パケットのデータを各部が相互にアクセスできる方法であれば本発明の一実施例に制限されることはない。

【0047】

【発明の効果】以上説明したように、本発明による暗号ゲートウェイ装置をフロントエンドプロセッサとして端末に接続して、端末間で通信されるパケット等の情報を受信し、情報の送信元と送信先とに応じて、暗号化、復号、又は非暗号化（通過）した情報を送信することにより、既存のAPや端末のハードウェアを改造することなく低コストで暗号通信システムを実現することができる。

【0048】さらに、本発明の暗号ゲートウェイ装置により、各端末間の通信を（暗号文又は平文、及び、同一グループ内又はグループ間を問わず）一切変更すること無く、暗号ゲートウェイ装置を設置したグループ間の通信文をすべて暗号化し、暗号ゲートウェイ装置を設置しないグループとの通信は平文のまま行うことができる。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

【図2】本発明の暗号ゲートウェイ装置を利用した暗号通信システムの概要を説明する図である。

【図3】本発明の一実施例によるシステム構成図である。

【図4】本発明の一実施例によるセッション鍵テーブルを説明する図である。

【図5】本発明の一実施例によるTCP/IP・LANの protocols を説明する図である。

【図6】本発明の一実施例によるパケット・フォーマットを説明する図である。

【図7】本発明の一実施例によるIPヘッダのフォーマットを説明する図である。

ットを説明する図である。

【図8】本発明の一実施例によるTCPヘッダのフォーマットを説明する図である。

【図9】本発明の一実施例による暗号化/復号処理のフローチャートである。

【図10】従来技術を説明する図（その1）である。

【図11】従来技術を説明する図（その2）である。

【図12】従来技術による暗号通信システムを説明する図である。

【符号の説明】

10、20、30、110 暗号ゲートウェイ装置

11、111 セッション鍵テーブル

12 テーブル管理手段

13 受信手段

14 受信情報解析手段

15 セッション鍵検索手段

16 暗号化/復号手段

17 送信手段

21<sub>1</sub>、...、21<sub>n</sub>、31<sub>1</sub>、...、31<sub>n</sub>、3

20 21、...、321 端末

40、42 伝送路

112 テーブル管理部

113、182 受信部

114 パケット解析部

115 セッション鍵検索部

116、184 暗号化/復号部

117、185 送信部

120 ネットワーク

130 端末1

132、142 アプリケーションプログラム

140 端末j

160 鍵配送センタ

162 セッション鍵

180、180<sub>1</sub>、180<sub>2</sub> 暗号ゲートウェイ装置

181 固定セッション鍵

183 受信情報解析部

【図4】

本発明の一実施例によるセッション鍵テーブル

セッション識別子				セッションID
送信元アドレス		送信先アドレス		
IPアドレス	ポート番号	IPアドレス	ポート番号	
IP <sub>1</sub> S <sub>1</sub>	P <sub>1</sub> S <sub>1</sub>	IP <sub>1</sub> D <sub>1</sub>	P <sub>1</sub> D <sub>1</sub>	K <sub>11</sub>
IP <sub>1</sub> S <sub>2</sub>	P <sub>1</sub> S <sub>2</sub>	IP <sub>1</sub> D <sub>2</sub>	P <sub>1</sub> D <sub>2</sub>	K <sub>12</sub>
⋮	⋮	⋮	⋮	⋮
IP <sub>n</sub> S <sub>1</sub>	P <sub>n</sub> S <sub>1</sub>	IP <sub>n</sub> D <sub>1</sub>	P <sub>n</sub> D <sub>1</sub>	K <sub>n1</sub>

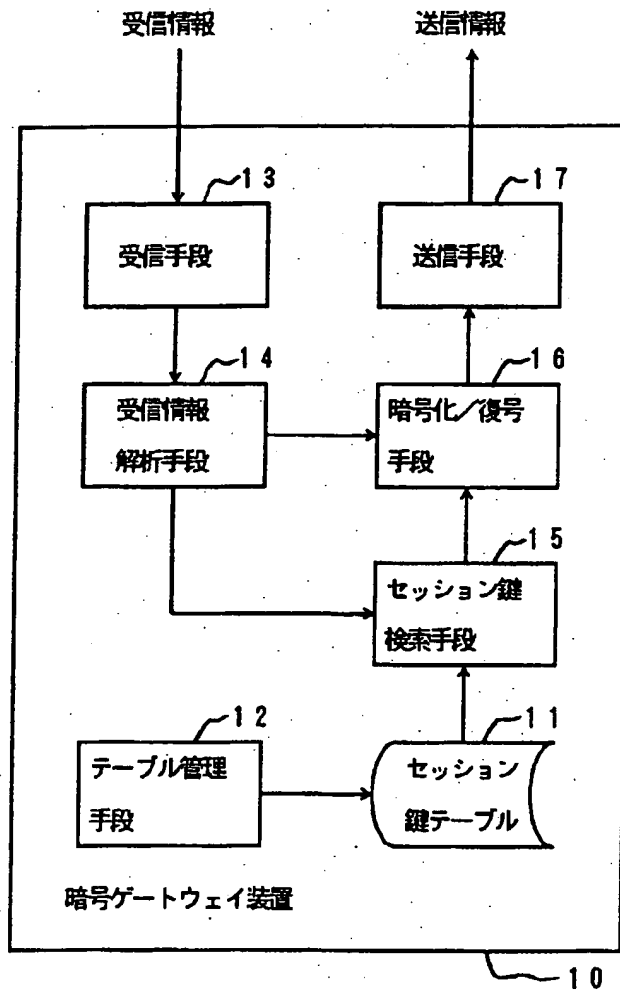
【図5】

本発明の一実施例によるTCP/IP・LANの protocols

上層レイヤ	AP
トランスポート	TCP
ネットワーク	IP
データリンク	MAC
物理	物理

【図1】

本発明の原理構成図



【図6】

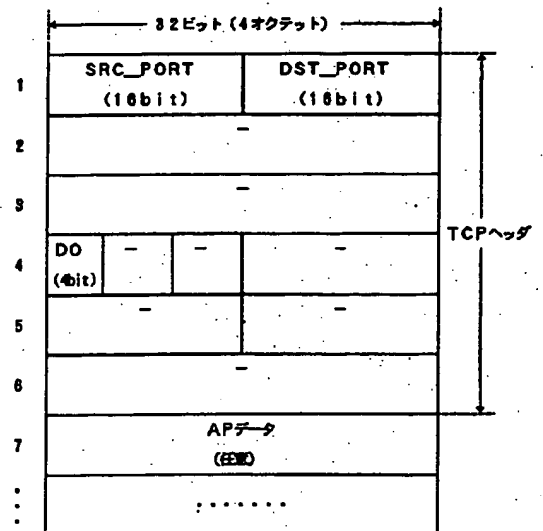
本発明の実施例によるパケット・フォーマット



MAC\_H: MACヘッダ  
 IP\_H: IPヘッダ  
 TCP\_H: TCPヘッダ  
 FCS: フレーム・チェック・シーケンス  
 [Shaded Area]: 暗号化領域

【図8】

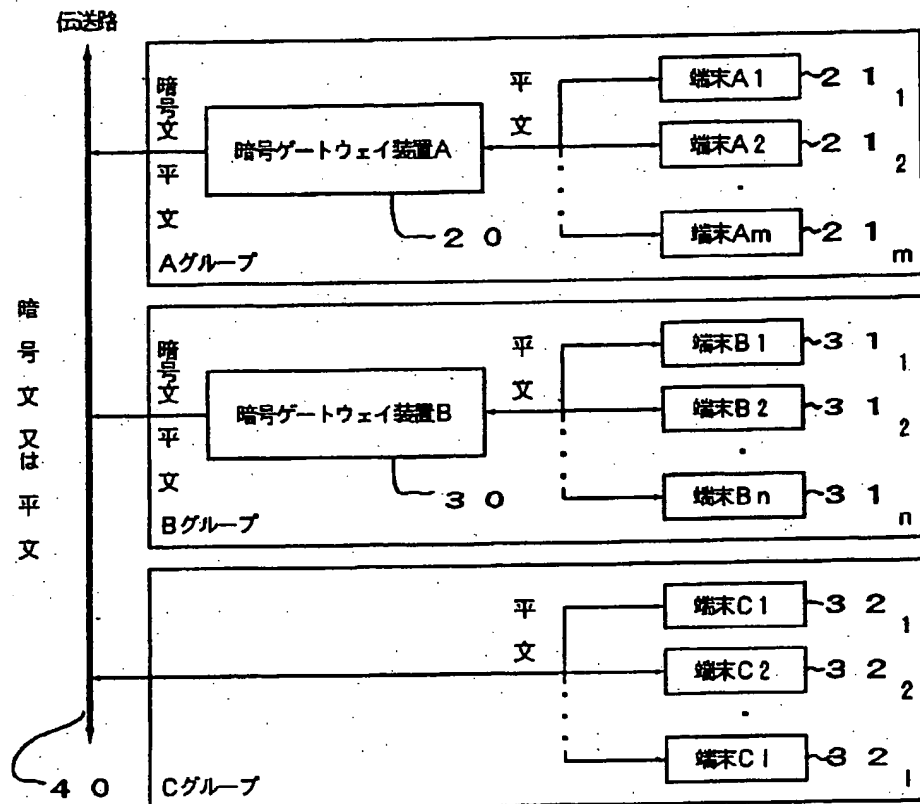
本発明の実施例によるTCPヘッダのフォーマット



SRC\_PORT: ソース・ポート  
 DST\_PORT: デスティネーション・ポート  
 DO: データ・オフセット

【図2】

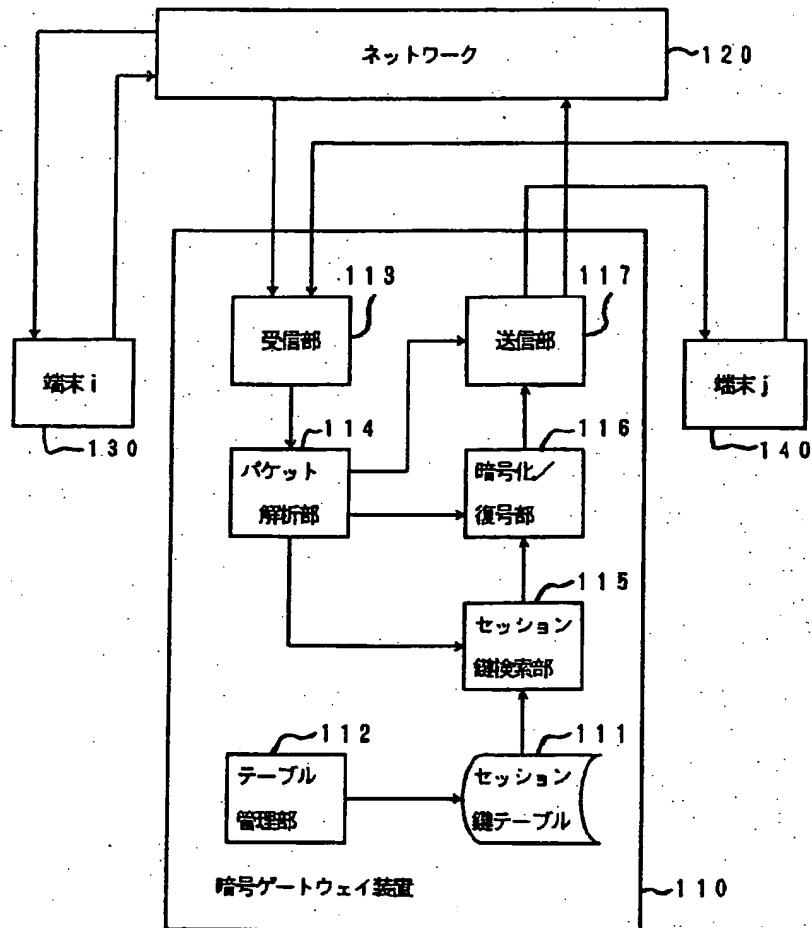
本発明の暗号ゲートウェイ装置による  
暗号通信システムの概説図





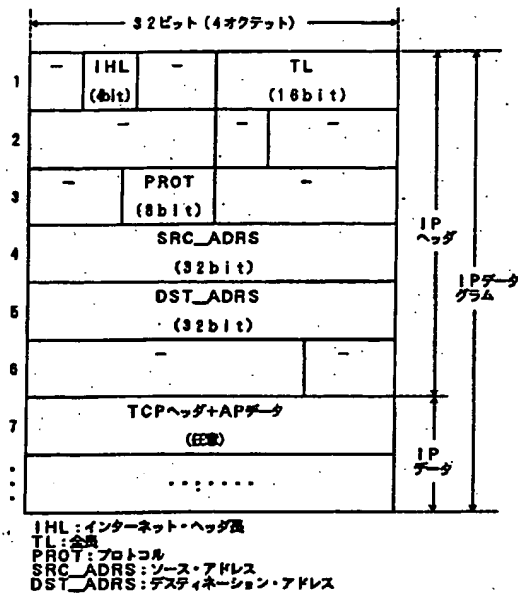
【図3】

本発明の一実施例によるシステム構成図



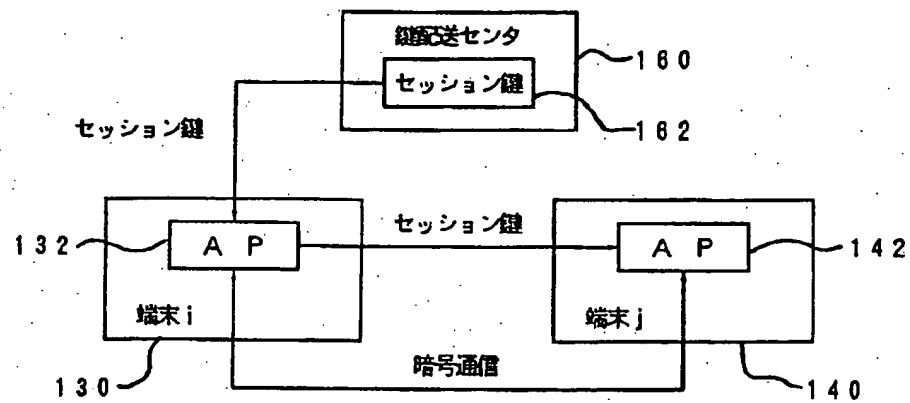
【図7】

本発明の一実施例によるIPヘッダのフォーマット



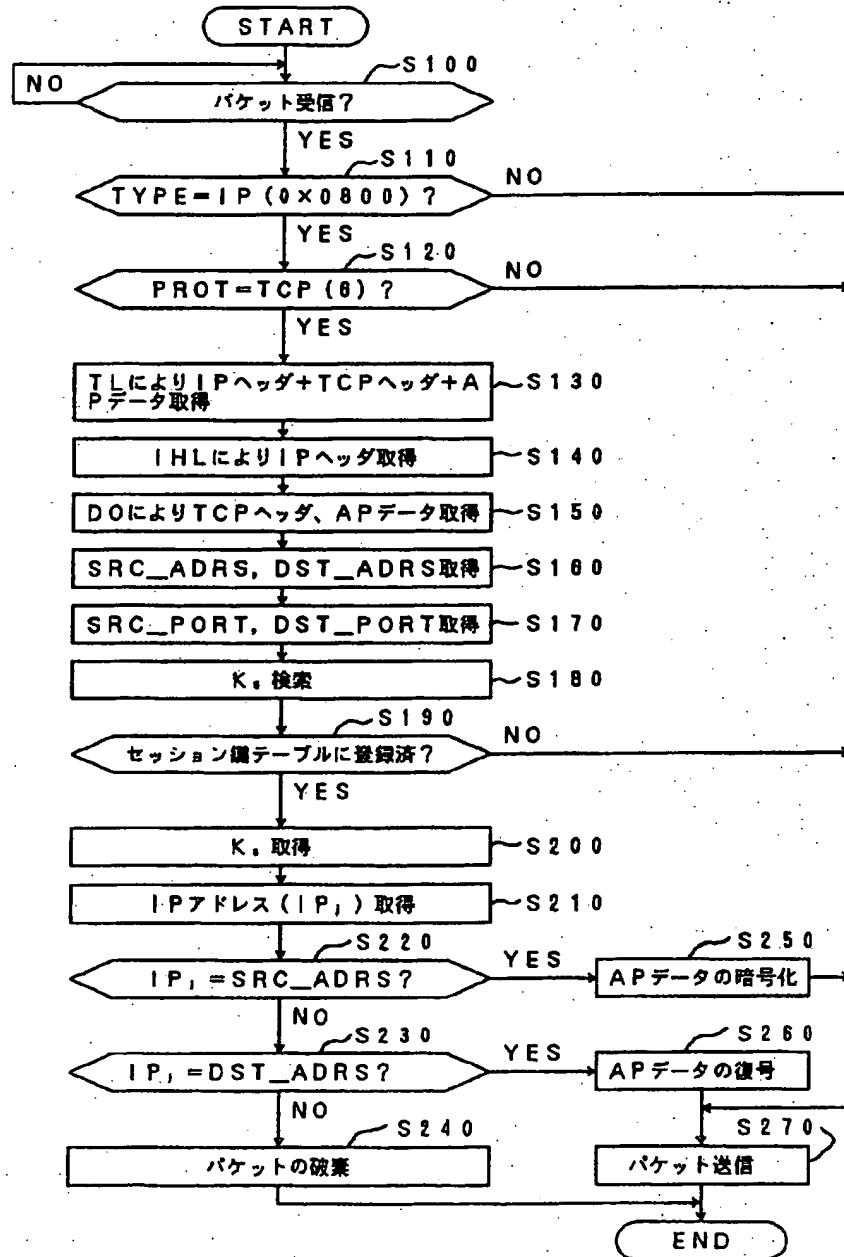
【図10】

従来技術の説明図(その1)



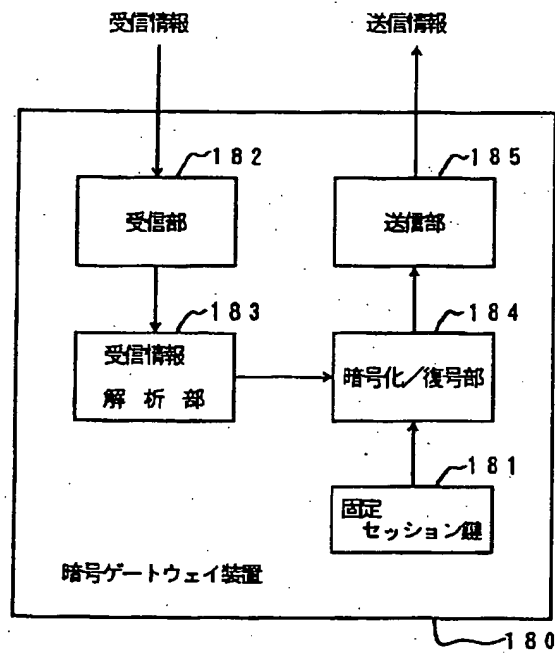
【図9】

本発明の一実施例による暗号化/復号処理のフローチャート



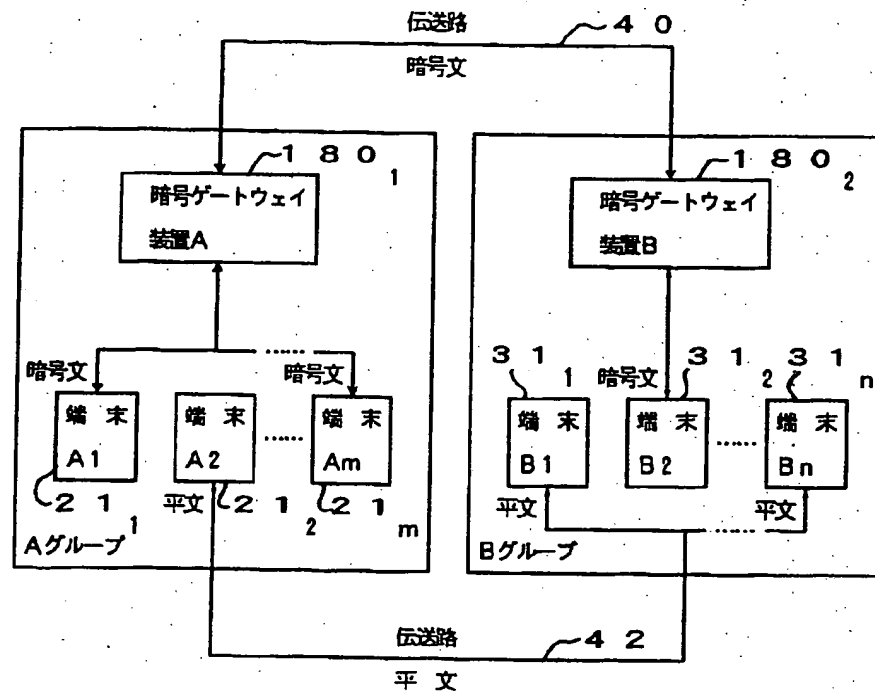
【図11】

従来技術の説明図(その2)



【図12】

従来技術による暗号通信システムの説明図



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**